GAU 2766
2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#10/B

In re Application of **Michael A. Epstein** Atty. Docket No.: **PHA 23,313**
Serial No.: **08/994,878** Group Art Unit: **2766**
Filed: **12/19/97** Examiner: **Ho S. Song**
Title: **ADMINISTRATION AND UTILIZATION OF PRIVATE KEYS IN A NETWORKED ENVIRONMENT**

12/20/00

RECEIVED
DEC 15 2000
Technology Center 2100

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

O I P E JC36
DEC 14 2000
PATENT & TRADEMARK OFFICE

**Amendment/Reply to Office Action**

Sir:

Enclosed is a reply in the above-identified application in response to the Office Action dated 11 September 2000.

Please replace the Abstract, in its entirety, with the following:

B'

The private and public keys of users, as encrypted with a symmetric algorithm by using individual user identifying keys are stored at a network server, indexed or addressable by user ID, and are sent to the user equipment only when needed. The user identifying keys are determined by hashing the users' respective passphrases or biometric information. After use, the private key and user identifying key are not retained at the user equipment. The encrypted private key is transmitted via the network to the user equipment along with a document to be approved by the user (in the case where the private key is used for digital signature) and, at the user equipment, the received encrypted private key is decrypted using a key determined at the user equipment by hashing either the user's passphrase, which is entered by the user, or the user's biometric information which is obtained by measurement or scanning the user. The received document is modified or merely reviewed, and a digital signature signifying the user's approval, is formed as a hash of the approved document encrypted using the user's private key. The digital signature and document are transmitted to the server, where verification takes place.

Please cancel claims 3, 4, 9, 10, 17, and 18.

Please amend the claims as follows. For convenience, a clean copy of each pending claim in this application is attached.

Sub C1

1. (Amended) A method of administration of private keys for a plurality of users for use to encrypt or decrypt items transmitted via a network, there being for each user a respective set of an ID, user identifying information, private key, and public key corresponding to the private key, said method comprising:

receiving via the network a user's ID;

reading from a storage means data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user; ~~and~~

sending via the network the encrypted private key, whereby the encrypted private key can be received and decrypted at the location of the user using the user's identifying ~~information.~~information;

receiving a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key; and

verifying the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document.

11. (Twice Amended) A system for administering private keys and corresponding public keys for a plurality of users, comprising:

computer readable storage means and

a server,

characterized in that:

the storage means includes therein respective IDs and encrypted private keys for the respective users which private keys have been encrypted using respective keys determined from respective user identifying information, and

the server is configured:

to read an encrypted private key from the storage means associated with an ID corresponding to a particular ~~user and~~user,

to transmit the encrypted private key to the particular ~~user.~~user,

to receive a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key, and

to verify the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document.

13. (Amended) A system as claimed in Claim 11, characterized in that there is further stored in the storage means the respective public keys corresponding to the private keys for the respective users.

14. (Amended) A system as claimed in Claim 12, characterized in that there is further stored in the storage means the respective public keys corresponding to the private keys for the respective users.